

Exhibit 39

SW-SEC00150761

From: Colquitt, Steven [/O=SOLARWINDS/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=0294A8D2FD6E40FA84FE5BAA92BC97CD-COLQUITT, STE]
Sent: 2/1/2018 4:33:28 PM
To: Pierce, Kellie [/o=SolarWinds/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=c60637762d9c4ea29729c77460571790-pierce, kelli]
CC: Johnson, Rani [/o=SolarWinds/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=61ad383fe3474bf084190056f2ce567b-johnson, rani]
Subject: RE: SDL Training
Attachments: SDL-AppSec-Training.pptx

Latest attached. Includes updated numbers for the 37 incidents.

From: Pierce, Kellie
Sent: Wednesday, January 31, 2018 2:36 PM
To: Colquitt, Steven <steven.colquitt@solarwinds.com>
Cc: Johnson, Rani <rani.johnson@solarwinds.com>
Subject: RE: SDL Training

Got it. I will set up a meeting early next week with Rani, as she wants to review the final materials. As we are reviewing implementation work of the MSP teams, they would like to be looped into the training. That being said, we need to loop August into the rollout for MSP. We can discuss this as well with Rani.
Thanks,
Kellie

From: Colquitt, Steven
Sent: Wednesday, January 31, 2018 3:30 PM
To: Pierce, Kellie <kellie.pierce@solarwinds.com>
Cc: Johnson, Rani <rani.johnson@solarwinds.com>
Subject: RE: SDL Training

No. I have made a few adjustments to help with flow. I am also updating the SDL graphic with SWi colors and few other graphical changes. I won't have that for a few more days. But for all intents and purposes, the content is the same

From: Pierce, Kellie
Sent: Wednesday, January 31, 2018 2:28 PM
To: Colquitt, Steven <steven.colquitt@solarwinds.com>
Cc: Johnson, Rani <rani.johnson@solarwinds.com>
Subject: SDL Training

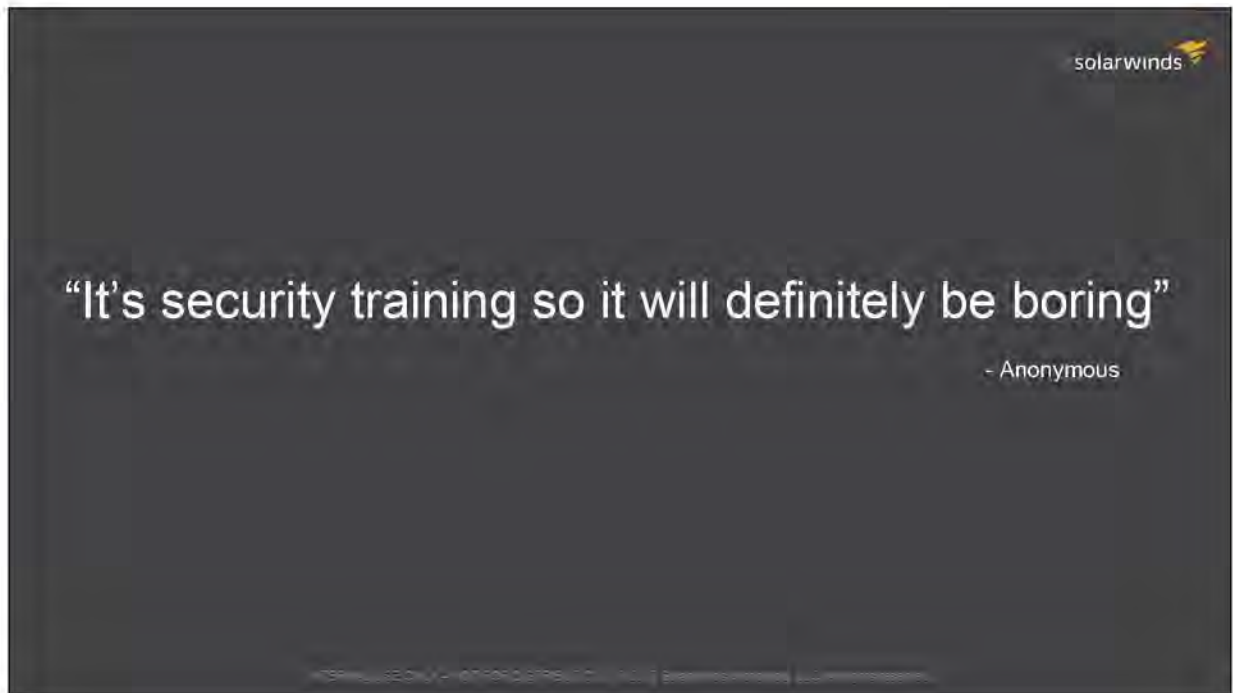
Hello Steven,
Is this your latest SDL training materials?
Thanks,
Kellie



Kellie Pierce | GDPR Project Manager | **SolarWinds**
Office: 512.498.6575

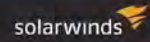


High-level SDL training (no operational content)
Bar (What we want to achieve over 2018)
We will be audited



This was said as a jest but in truth, security can be perceived as boring and a burden with overhead that will slow teams down; more "things" we have to do. But I believe we are approaching security in a pragmatic manner so that it won't be heavy process that disrupts our development.

Agenda

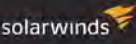


- What is an SDL?
- Why do we need an SDL?
- The SolarWinds SDL
- The activities
- Q&A



INTERNAL USE ONLY – NOT FOR DISTRIBUTION © 2017 SolarWinds Worldwide, LLC. All rights reserved.



Secure Development Lifecycle

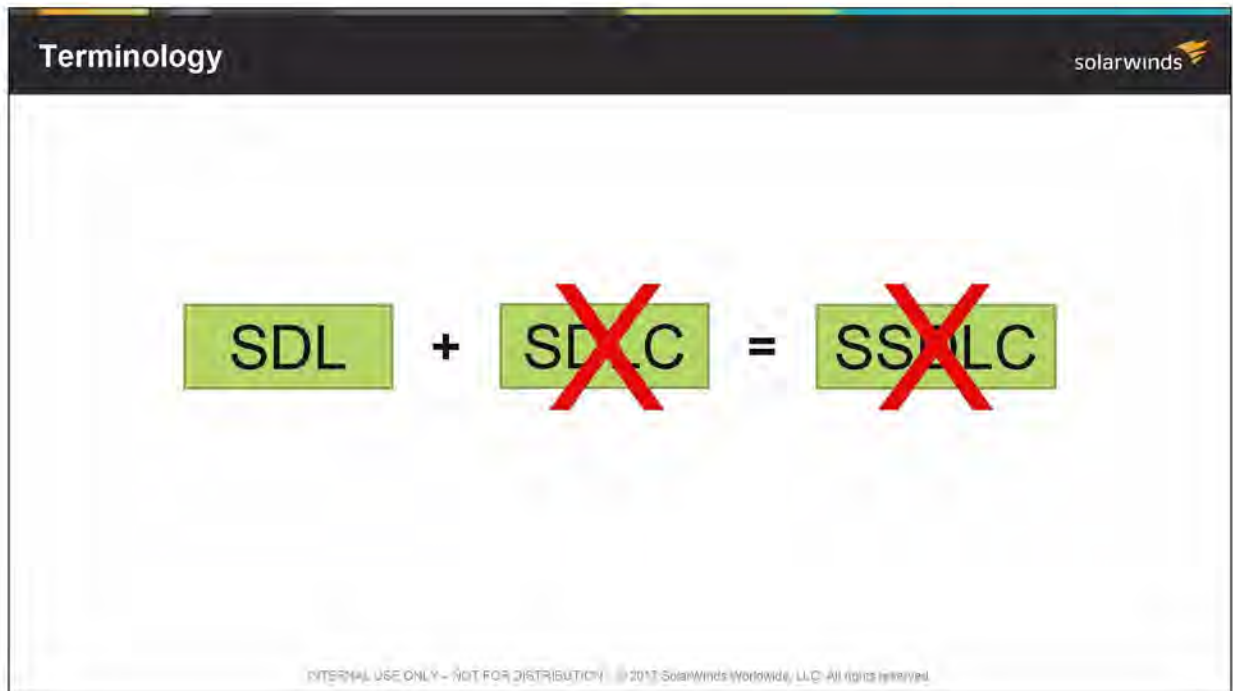
What is a Secure Development Lifecycle?

SDL – a set of repeatable activities that builds security into our SDLC: *Security by Design*

INTERNAL USE ONLY – NOT FOR DISTRIBUTION © 2017 SolarWinds Worldwide, LLC. All rights reserved.

These activities help us focus security throughout the lifecycle of application development. This enables us to design, build and ship more secure software. It give us the opportunity to think through the potential risks and make calculated decisions about mitigations and acceptable levels of risk. While no application is 100% secure, we can be more confident that we are shipping secure software.

A Secure Development Lifecycle
Enables the construction of secure software
Supports Security by Design
Repeatable security activities
Prioritizes security and privacy
Defines checkpoints
Provides oversight
Improves engineering efficiency
Reduces costs – earlier detection



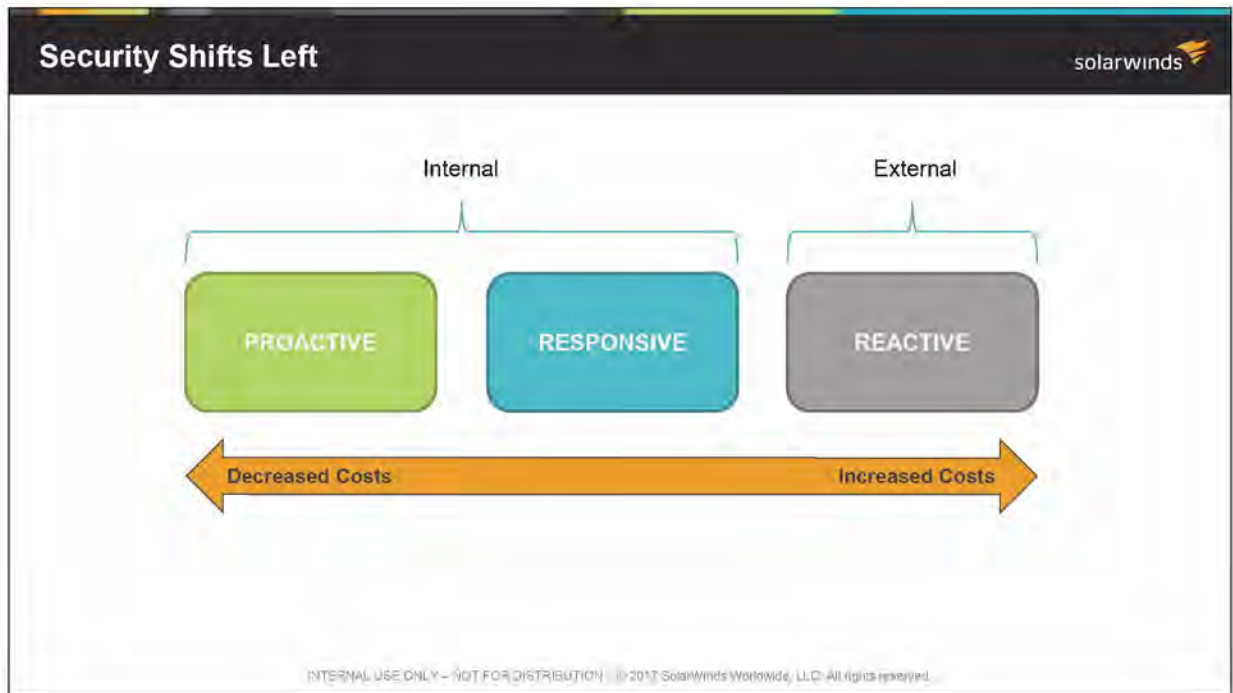
SDL - Secure Development Lifecycle - this is a set of repeatable activities that are applied to software development to create secure products

+

SDLC - Software Development Lifecycle - this is a set of repeatable activities that produces software

=

SSDLC - Secure Software Development Lifecycle - all activities enable engineers to produce secure software.



Applying an SDL shifts security left





We started tracking incidents mid Q1 of this year. These are externally reported incidents that then required us to initiate the incident response plan.



Every time we have to react to a security incident there is a time and financial cost.

Incidents have time and financial costs associated

Costing exercise

131 hours start to remediate

Lost opportunity *

No renewal due to vulnerabilities

Total cost of 2017 incidents

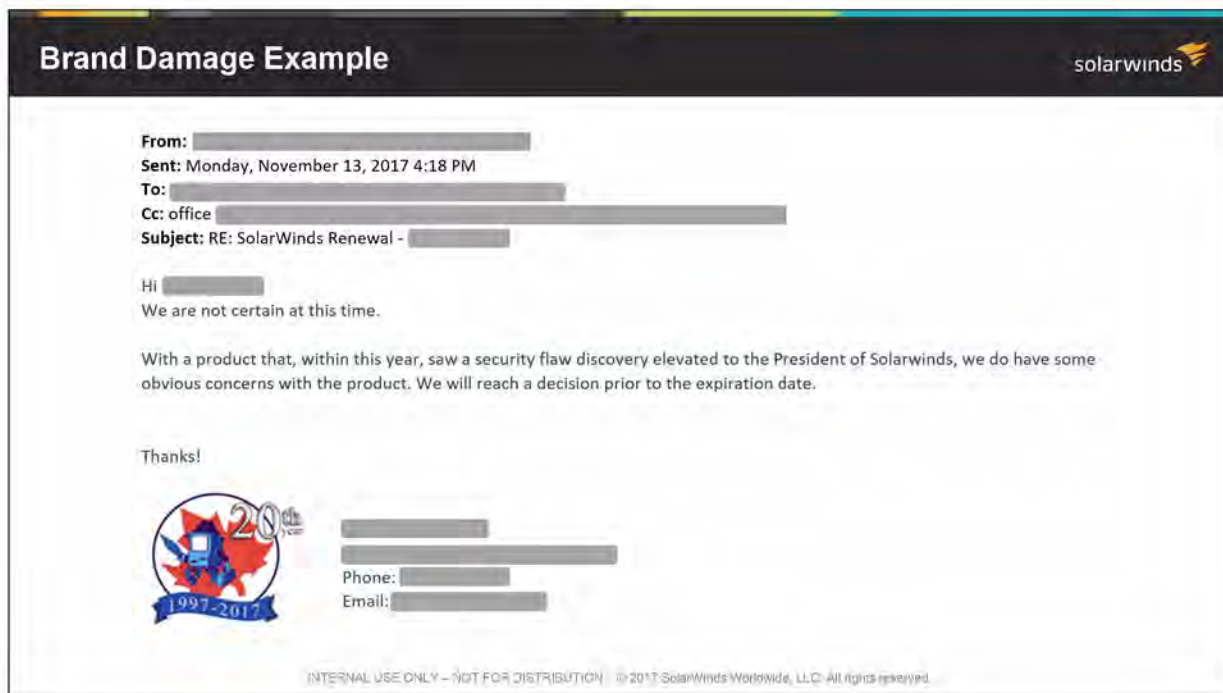
(Time * Cost) + Lost Opportunity

Extrapolated loss over 3 years... \$570

We are building new products this year. How much time has been spend thinking about the security and privacy considerations?



Most of you strongly agree that our customers expect Swi software to be secure.



This is an reply from a customer to an email sent to inquire about renewing a product. Their response....



<https://gdpr-info.eu/art-25-gdpr/>
<https://gdpr-info.eu/art-32-gdpr/>

'The controller shall..implement appropriate technical and organisational measures..in an effective way.. in order to meet the requirements of this Regulation and protect the rights of data subjects'

Art. 25

Data protection and privacy by design and by default

Art. 32


encryption of personal data;

ensure the ongoing confidentiality, integrity, availability


ensuring the security of the processing [of data]

GDPR Compliancesolarwinds

Defensible



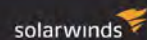
Demonstrable



INTERNAL USE ONLY – NOT FOR DISTRIBUTION © 2017 SolarWinds Worldwide, LLC. All rights reserved.

We must be able to defend our processes as secure
We must be able to demonstrate how we apply security

An SDL will help us:



Reduce the number of security incidents

Protect our brand

Meet security expectations

Comply with GDPR privacy laws

INTERNAL USE ONLY – NOT FOR DISTRIBUTION © 2017 SolarWinds Worldwide, LLC. All rights reserved.

THE SWi SDL?

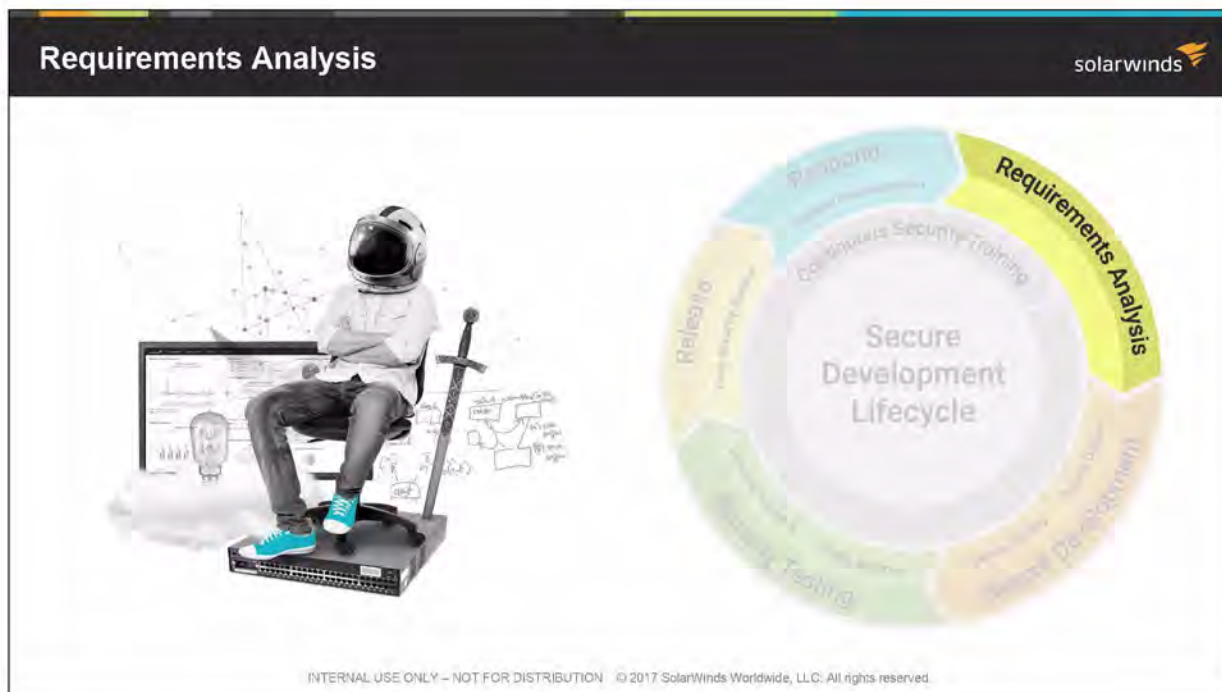


In a repeatable fashion, focus is applied to each of the following security activities during development:

Security Training
 Requirements Analysis
 Secure Development
 Secure Design
 Secure Coding
 Security Testing
 Static Analysis
 Dynamic Analysis
 Release
 Final Security Review
 Respond
 Incident Response Plan



Security awareness
Security best practices
Industry standards
Secure design
Secure coding
Security testing



What are we building?
What are the security requirements?
What are the privacy constraints?
How will these effect development and testing?
Ex., define security test cases based on requirements analysis



Secure Design

3rd party components

Using latest?

Are there known vulnerabilities?

Cryptography requirements

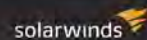
Privacy considerations

Authentication and access

Reducing the attack surface – do we understand the risks?

Threat modeling

What's Wrong?



```
HRESULT GetMachineName(  
    WCHAR *pwszPath,  
    WCHAR wszMachineName[MAX_COMPUTERNAME_LENGTH_FQDN+1])  
{  
    pwszServerName = wszMachineName;  
    LPWSTR pwszTemp = pwszPath + 2;  
    while ( *pwszTemp != L'\\' )  
        *pwszServerName++ = *pwszTemp++;  
    /* ... */  
}
```

INTERNAL USE ONLY - NOT FOR DISTRIBUTION © 2013 SolarWinds Worldwide, LLC. All rights reserved.

3.37 million support calls



Secure Coding

Leverage best practices

OWASP (Top 10)

SANS (25)

SEI – CERT

Best practices such as:

Error Handling

Authentication and Access Control

Session Management

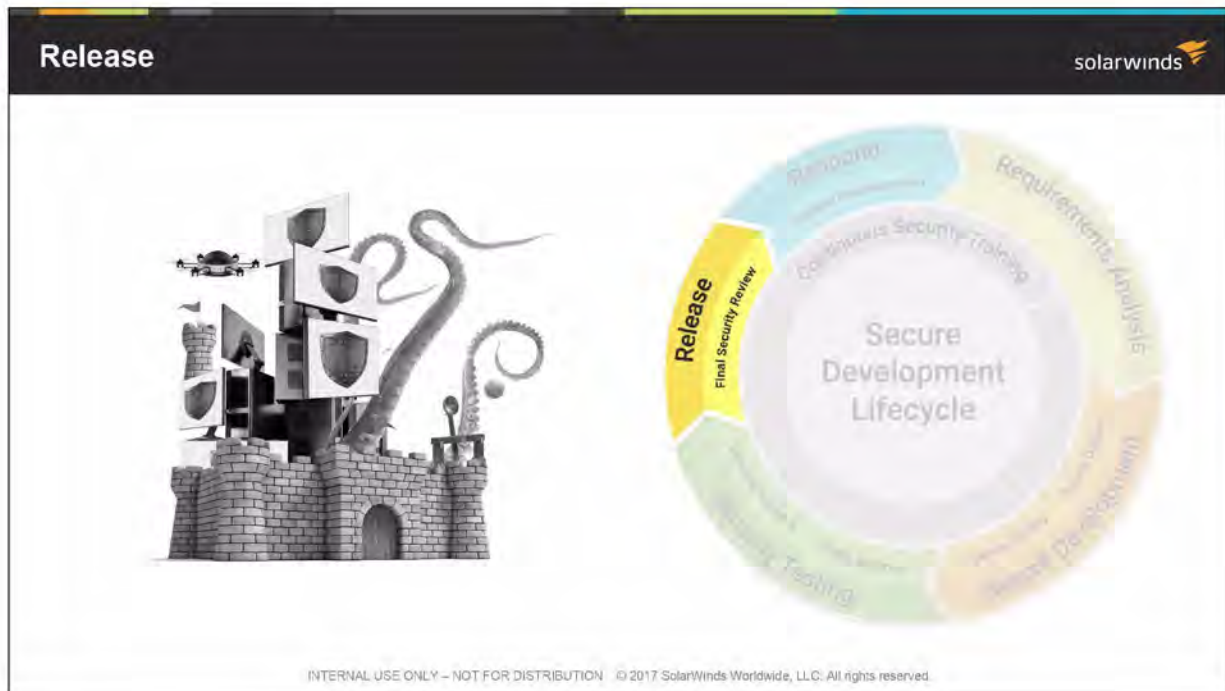
Handling input and output

Data protection (privacy)



Static Analysis (SAST)
Evaluates the source code
Supports Shifts security left

Dynamic Analysis (DAST)
Evaluates the running program
Vulnerability scanning
Penetration testing
Fuzz testing



Final Security Review
Reviews collateral
Threat models, security testing output, security test cases
Establishes security and privacy confidence level



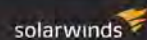
Incident Response Plan
Established process for response
Ensures the right people engaged at the right time
Manages prioritization and timelines
Manages communication
Provides tracking



In a repeatable fashion, focus is applied to each of the following security activities during development:

- Security Training
- Requirements Analysis
- Secure Development
- Secure Design
- Secure Coding
- Security Testing
- Static Analysis
- Dynamic Analysis
- Release
- Final Security Review
- Respond
- Incident Response Plan

Next steps



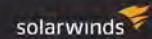
- Train and operationalize for Core IT, MSP and Cloud teams

- Pragmatic approach
- Pilot implementation
- Adjust



INTERNAL USE ONLY - NOT FOR DISTRIBUTION © 2011 SolarWinds Worldwide, LLC. All rights reserved.

References and Resources



External References

- Microsoft
 - SDL: <https://www.microsoft.com/en-us/SDL>
 - Threat Modeling Tool: <https://www.microsoft.com/en-us/download/details.aspx?id=43168>
- SANS:
 - TOP 25: <https://www.sans.org/top25-software-errors/>
 - <https://software-security.sans.org/resources/swat>
- OWASP
 - Top 10 2017: https://www.owasp.org/images/7/72/OWASP_Top_10_2017_%28en%29.pdf.pdf
 - Secure Coding: https://www.owasp.org/images/0/08/OWASP_SCP_Quick_Reference_Guide_v2.pdf
 - Secure Testing: <https://www.owasp.org/images/1/19/DTGv4.pdf>
 - Threat Modeling: https://www.owasp.org/index.php/Application_Threat_Modeling
- Web Application training
 - <https://aem.globalsight.com/library/courses/webappsec101-fms/1a0e0f0a0e0e>
- GDPR: <https://www.eugdpr.org/the-regulation.html>

Internal References

- <https://cp.solarwinds.com/display/SAI/RO/Cyber+Security+--+Learning+Material>
- <https://cp.solarwinds.com/display/Eng/Security+Portal>
- <https://cp.solarwinds.com/display/Eng/Peer+To+Peer+--+Security+Training>
- SolarWinds Secure Development Lifecycle – Core IT
 - <https://cp.solarwinds.com/display/Eng/Secure+Development+Lifecycle>

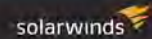
INTERNAL USE ONLY – NOT FOR DISTRIBUTION © 2017 SolarWinds Worldwide, LLC. All rights reserved.

Q&A



Backup

Core IT Engineering Security Phase Matrix



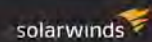
SWI CORE IT PHASE	SDL PHASE	ACTIVITIES	ASSERTION
Planning	Requirements Analysis	<ul style="list-style-type: none"> Determine security requirements Determine privacy constraints 	Product Architect
Development and Testing	Secure Design	<ul style="list-style-type: none"> Threat modeling (TM) Attack surface reduction (ASR) Establish security & privacy design requirements 	Product Architect
	Secure Coding	<ul style="list-style-type: none"> Apply secure design principles Apply secure coding principles 	Engineering Manager
	Static Analysis	<ul style="list-style-type: none"> Leverage static analysis tool 	
	Dynamic Analysis	<ul style="list-style-type: none"> Vulnerability scanning Penetration testing 	
Regression	Final Security Review	<ul style="list-style-type: none"> Review of threat model and ASR Review security test scans output 	Product Architect

Overlap

Iterative

INTERNAL USE ONLY - NOT FOR DISTRIBUTION © 2013 SolarWinds Worldwide, LLC. All rights reserved.

Secure Coding – OWASP Top 10 2017



- Injection
- Broken Authentication
- Sensitive Data Exposure
- XML External Entities
- Broken Access Control
- Security Misconfiguration
- XSS
- Insecure Deserialization
- Using Components with Known Vulnerabilities
- Insufficient Logging & Monitoring

INTERNAL USE ONLY - NOT FOR DISTRIBUTION © 2017 SolarWinds Worldwide, LLC. All rights reserved.



Software centric approach to TM

What are we building?
Deconstruct the application
Where are the risks?
Identify the trust boundaries
Entry points
What data or control exchanged between entities
How do we mitigate or eliminate the risks?
What technical controls can we add to reduce the impact and likelihood?
How can we design security controls that will prevent a vulnerability?

Risk = Likelihood * Impact

STRIDE - Microsoft
Spoofing
Tampering
Repudiation
Information Disclosure
Denial of Service
Elevation of Privilege

Microsoft Threat Modeling Tool - <https://www.microsoft.com/en-us/download/details.aspx?id=49168>

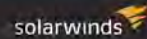
Secure Coding

solarwinds

```
+= " where ALERTID=" + alertId;
```

INTERNAL USE ONLY - NOT FOR DISTRIBUTION © 2013 SolarWinds Worldwide, LLC. All rights reserved.

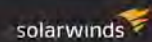
Secure Coding – CERT Secure Coding (C++, Java)



- Declaration and initialization
- Expressions
- Integers
- Containers
- Characters and strings
- Memory management

INTERNAL USE ONLY - NOT FOR DISTRIBUTION © 2013 SolarWinds Worldwide, LLC. All rights reserved.

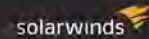
Secure Coding – Web Application Best Practices



- Error handling and logging
 - Handle exceptions properly and generically
 - Log authentication activities
- Authentication
 - Store credentials securely
 - Run with minimal permissions
- Access control
 - Apply the principle of least privilege

INTERNAL USE ONLY - NOT FOR DISTRIBUTION © 2013 SolarWinds Worldwide, LLC. All rights reserved.

Secure Coding – Web Application Best Practices



- Data protection
 - Secure data at rest and in flight
- Session management
 - Ensure sufficient entropy with tokens and identifiers
 - Implement session timeouts
- Handling input and output
 - Apply contextual encoding
 - Use parameterized queries
 - Validate all input

INTERNAL USE ONLY – NOT FOR DISTRIBUTION © 2013 SolarWinds Worldwide, LLC. All rights reserved.